Notice of Allowability	Application No.	Applicant(s)	
	10/071,328	GLADSTONE ET AL.	
	Examiner	Art Unit	
	Benjamin Buss	2129	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *papers filed 4/16/2007*.

2. ☒ The allowed claim(s) is/are *11-14,21-24 and 26-35*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☒ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20070606* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Christopher Lutz (Reg. No. 44,883) on 6/6/2007.

The application has been amended as follows:

Claim 11, lines 23-24: Changed "the monitoring process operable to implement the decision to block or allow the identified activity" to

-- the monitoring process operable to:

operate in a state collection mode, the state collection mode operable for gathering normal patterns of activity;

subsequently operate in a lockdown mode, the lockdown mode operable to detect and distinguish predetermined patterns of events and the gathered normal patterns of activity;

identify detected patterns as unsafe based on user selection; and

implement the decision to block or allow the identified activity --.

Claim 21: Changed "The method of claim 11 wherein stateful reference monitor computes" to -- The computer-implemented reference monitor of claim 11 further computing --.

Claim 22: Changed "The method of claim 21" to -- The computer-implemented reference monitor of claim 21 --.

Claim 23: Changed "The method of claim 22 wherein stateful reference monitor is" to -- The computer-implemented reference monitor of claim 22 --.

Claim 24: Changed "The method of claim 23" to -- The computer-implemented reference monitor of claim 23 --.

Claim 25: Canceled.

Claim 27, line 4: Changed "stored state" to -- stored real-time state --.

Claim 27, line 10: Changed "state" to -- real-time state --.

Claim 27, line 13: Changed "a set of rules" to -- the plurality of rules --.

Claim 27, line 21: Changed "the set of rules" to -- the plurality of rules --.

Claim 27, lines 25-26: Changed "the monitoring process operable to implement the decision to block or allow the identified activity" to

-- the monitoring process operable to:

operate in a state collection mode, the state collection mode operable for gathering normal patterns of activity;

subsequently operate in a lockdown mode, the lockdown mode operable to detect and distinguish predetermined patterns of events and the gathered normal patterns of activity;

identify detected patterns as unsafe based on user selection; and

implement the decision to block or allow the identified activity --.

Specification

Page 4, line 30: Changed "software produce" to -- software product --.

Title: The title has been changed to: "ACCESS CONTROL BY A REAL-TIME STATEFUL REFERENCE MONITOR WITH A STATE COLLECTION TRAINING MODE AND A LOCKDOWN MODE FOR DETECTING PREDETERMINED PATTERNS OF EVENTS INDICATIVE OF REQUESTS FOR OPERATING SYSTEM RESOURCES RESULTING IN A DECISION TO ALLOW OR BLOCK ACTIVITY

IDENTIFIED IN A SEQUENCE OF EVENTS BASED ON A RULE SET DEFINING A PROCESSING POLICY".

Drawings

2. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the informal drawings filed 2/8/2002 are difficult to read and the lined paper used makes the scanned images unsuitable for publication. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Reasons for Allowance

3. The following is an examiner's statement of reasons for allowance:

Claims 11-14, 21-24, and 26-35 are considered allowable since when reading the claims in light of the specification, as per MPEP §2111.01 or In re Sneed, 710 F.2d 1544, 1548, 218 USPQ 385, 388 (Fed. Cir. 1983), none of the references of record alone or in combination disclose or suggest the combination of limitations specified in the independent claims including a plurality of interceptors for identifying the activity (supported at e.g., pg. 5 lines 1-20 and pg. 8 line 30 – pg. 9 line 23), stored real-time state information (supported at e.g., pg. 4 lines 26-32), a state collection mode operable for gathering normal patterns of activity and a lockdown mode operable to detect and distinguish predetermined patterns of events and the gathered normal patterns of activity (supported at e.g., pg. 12 line 28 – pg. 13 line 15), and identifying detected patterns as unsafe based on a user selection (supported at e.g., pg. 12 line 28 – pg. 13 line 15 and pg. 15 lines 12-13 and pg. 19 lines 19-27) as specified in claims 11, 26, and 27.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Correspondence Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin Buss whose telephone number is 571-272-5831. The examiner can normally be reached on M-F 9AM-5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Vincent can be reached on 571-272-3080. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin Buss
Examiner
Art Unit 2129

/BB/

DAVID VINCENT
SUPERVISORY PATENT EXAMINER